

METHOD AND SYSTEM FOR SECURING ENABLEMENT ACCESS TO A DATA SECURITY DEVICE

ABSTRACT OF THE DISCLOSURE

An embedded security subsystem, and method for implementing the same, which provide secure controllability of a data security device within a data processing system. The embedded security subsystem of the present invention includes a persistent enable flag for providing control access to the data security device, wherein the persistent enable flag is accessible only in response to a power-on reset cycle of the data processing system. The persistent enable flag is read-only accessible to runtime program instructions. A pending state change flag that is write accessible by runtime program instructions is utilized for setting an intended next state of the persistent enable flag such that control access to the data security device is enabled only during a subsequent power-on reset of said data processing system.